* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] About computer system, a global positioning system (GPS) is used especially for this invention for a country / local check, and it relates to the computer system which can permit the encryption function of a computer, and its approach.
[0002]
[Description of the Prior Art] GPS is the set of two or more satellites which the American government holds, and offers positional information and navigation information very with high precision by worldwide one for 24 hours. By hearing three or more satellites, a GPS receiver can detect an own exact location. Although it is a very exact system with wide range and GPS, other satellite positioning systems exist. The American government imposed fetters on U.S. hi-technology business by forbidding export of important encoding technology in 1997. Thereby, compared with the competition company of the foreign country where sale of encoding technology is not restricted legally, as for an American company, the sales amount is decreasing considerably. Reduction of such the sales amount is produced also by tapping of monopolistic business information, and powerful encoding technology is exported, and such business information should fully be protected, when it is wide range and is used.
[0003] However, only the United States does not necessarily have the restrictive law. For example, France has forbidden import of an encryption product, unless the license has been acquired, and this license is not acquired simply. Russia, China, Brazil, Singapore, etc. can be raised as other countries which have the restrictive law. Export of equipment similar to a high performance computer and it has also restricted the law about export of the U.S. However, in more than the level which the throughput of this equipment specifies to a computer theoretical (theory) performance (CPT) criterion in this case, export is restricted. Exporting the system which has current and 200 or more CPT to many foreign countries is forbidden. However, it is considered that such a CPT criterion will stop catching up with a high-end workstation and a home computer immediately when the throughput of today's small computer increases by leaps and bounds.
[0004] Other problems produced with the law of export restrictions are the points which cannot control downstream transfer (down-stream transfer) effectively. That is, there is a danger that the system exported to the permitted foreign country will be again exported to the foreign country of disapproval while a manufacturer does not know. The limit about export is not only troublesome, but changes. For example, when Commerce Department was able to carry out the demonstration of the process for a U.S. commercial enterprise to develop a key restoration product recently, this company proposed that the 56-bit encryption product of a Data Encryption Standard (DES) could be exported. However, when a key restoration product is introduced, the government is requiring that this processing should be exhibited, when key restoration processing is guaranteed. For a certain customer, providing other companies etc. with a key will produce a risk -- the confidentiality of a key will be spoiled -- from this company. Therefore, the demand of the government is the cause of reducing technical development volition.
[0005] Other well-known encryption products are Pretty Good Privacy (PGP), and this offers the code to

2048 bits. This is a kind of open key product, and does not need conversion of a privacy key in transmission of a message. PGP has the powerful algorithm in both license and message transmission. A transmitting side enciphers a message using the unique open key which a receiving side can exhibit freely. In a receiving side, in order to decode a message, an unique privacy key is used for this receiving side. As for those who are possible also for enciphering a message using the privacy key of a transmitting side, and know the open key of a transmitting side by this, anyone can decode a message. This is an important thing in order to generate the digital signature currently widely used in business dealings and individual dealings. Suggestion is given to U.S. Pat. No. 5635940 about location dependence actuation of a modem (Hickman etc.). This United States patent is indicating the modem including the device for determining the location of a modem. Depending on a location, configuration of the communication link part of equipment will be carried out again, and it will be in an established state required for actuation in the location.

[0006]

[Summary of the Invention] The computer system of this invention enables alternative control of an encryption engine / algorithm according to the related limit law using the GPS hardware provided for the check of a country/area. The advantage of the system of this invention is that a license key is controllable by the location distant from the end user. For example, it judges whether the software encryption application installed in the computer acquires GPS information from GPS hardware, and is in the location which the location of a system can permit, in view of the specific level of encryption. Exact reading of a user location can be performed using GPS. The use is restricted for the specific encryption product provided in the machine only for example, in the U.S., and when the location where it was recognized by GPS is in the U.S., encryption is permitted on powerful level. However, when it judges that an encryption product exists in the location where encryption on powerful level is not approved, an encryption function is impossible-ized so that a functional down may be carried out automatically or it may agree in an export-restrictions convention of a federation.

[0007] Other advantages of the system of this invention are being able to use it in order to control the downstream transfer of the powerful computer by which export is restricted. For example, export is restricted to the country of some specification [the computer which has two or more processor capacity which is beyond maximum capacity]. When the computer which has such capacity is located in domestic [of disapproval], the capacity of a processor falls to the level corresponding to law, or is impossible-ized. The advantage of further others of this invention is that the user of a specific location can install the software application specified by the computer manager of this organization in a systematic customer.

[0008] In a suitable example, the U.S. export license demand should just agree in monotype license. Since, as for the security function with the above-mentioned location dependency, the software (or hardware) limited to location data makes it impossible to operate in the forbidden location, even if the software (or hardware) which cannot operate may be incorporated in the system, the software (or hardware) which can operate will be exported. Therefore, once a certain type of license is issued, each license of the upgrade product (or new peripheral device of location dependence) of the software of location dependence is not needed. Therefore, the upgrade (or new peripheral device) of software will be quickly sold to a market.

[0009]

[The mode of implementation of invention] In order to offer exact positional information, the GPS system was constituted so that it might be first used by the army. The GPS product was used by the army, in order to detect the soldier of a battlefield, and the location of equipment, and to follow those migration, and to report to a marine naval ship and to provide the airplane of an army with positional information and navigation information. The GPS product is developed as many objects for commercial applications today. As commercial application, a survey and mapping, the air and marine navigation, a car tailing system, a mobile computer, a cellular platform, etc. can be raised.

[0010] Even if it uses a very highly precise atomic clock, a certain kind of error will arise in the process of spotting. Furthermore, Selective Availability It is the program created by the Department of Defense

of the U.S., and (SA) is the security purpose, and to the user who is not an army, intentionally, this program is making it rather than it has so exact GPS. By having used SA, the accuracy of a location is the accuracy of 30-100-meter range extent. Even when not using SA, other errors will arise. The most serious thing among these errors is based on fluctuation of the ionized layer of the earth, and fluctuation of this ionized layer affects the rate of a GPS radio signal. Other causes of error generating are based on the steam in the stratum on the front face of the earth. These errors are both very small. The precision of GPS improves by reading the reference signal from the DGPS beacon receiver fixed to near using a differential GPS (DGPS) function.

[0011] If it says simply, the interaction between software and hardware will be performed by the following approaches as shown in drawing 1 and drawing 2 . First, a user acts to a system as powering on. POST processing of a system is performed and the condition of all hardware is checked. Especially, when a GPS receiving circuit is operating state, GPS data are processed and stored and it stands by that software is performed and a demand is generated. When not receiving a software demand, a hardware firmware program checks a software demand continuously. Then, if software is loaded completely and an encryption program is performed, the loop-formation processing which checks that the software demand was transmitted to hardware and this demand has been transmitted will be started. Hardware's reception of a software demand confirms whether processed this demand and this demand was attested. Encryption is permitted when the demand is attested. what kind of reason -- be -- a hardware firmware will determine shut [software / the program which requires effective positional information], if it reports to software that the location which is not effective was detected.

[0012] Drawing 1 shows the GPS hardware flows of control for starting encryption from powering on. In step 100, GPS equipment begins power-up, i.e., by acting as powering on, and this processing checks the condition of all systems in step 105. When the system of arbitration reports failure generating after power-up, processing impossible-izes encryption of the arbitration of step 110. When it is reported that all systems can operate, in step 115, the location of a specific transmitter is checked and transmitted by the GPS system. After a location is transmitted, in step 120, a system stands by the application demand (APP demand) signal from a user. And in step 125, if it judges with the demand not being received yet, processing will perform this loop-formation processing until it returns to step 105, it performs a status check and a demand is received from a target, i.e., a user. A demand is pretreated in order to detect whether a demand is an effective demand in step 130, if a demand is received. And in step 135, if judged with a demand not being effective, it will return to step 105 and repetitive activation of the step which performed the status check and described above will be carried out. When a demand is effective, an authorization code is returned to a target, and encryption of application is permitted and performed in step 140. A processing loop formation checks continuously whether it can be continued with a predetermined time interval, the condition of a target can be updated, and a target can operate.

[0013] Drawing 2 is a software algorithm performed between authentication processings. The condition (APP condition) of application is checked and it is made to be appropriately processed in step 200. In step 205, software requires the hardware to GPS hardware. In step 210, when GPS hardware judges with actuation being impossible, it shifts to step 215 and a target unit judges that the GPS system is not used. However, except for the specific function of encryption or others, restricted actuation is performed in this case. GPS hardware is detected, when it can operate, it progresses to step 220 and a suitable software option is chosen for a specific target unit. And in step 225, in order to transmit to a master unit, a demand is transmitted to hardware. In step 230, when it judges with the demand having been processed appropriately, this processing is ended, and when not processed, a error handling routine is performed in step 235.

[0014] Drawing 3 shows the portable computer system which performs the new encryption approach of this invention. The system is equipped with the power converter 305 which charges a dc-battery. It is desirable to provide the dc-battery interface (I/F) 310 between a dc-battery and other circuits. Power is supplied through a full wave rectifier (FWR) 300 from AC main power supply, and the power converter 305 provides a dc-battery 315 with DC electrical potential difference. A dc-battery 315 (or converter 305) supplies DC power supply Vdd to a portable computer system through a voltage regulator 320. The

portable computer system is equipped with the following components.
[0015] - User input device (a keyboard 335 and mouse 340)
- At least one microprocessor 325[this microprocessor receives an input from an input device through the interface-management chip 330. In addition, an interface-management chip also offers the interface to various ports.]
- Memory with an accessible microprocessor (a flash memory 355 and RAM360)
- The data output device which outputs the data which the microprocessor generated (a display 350 and video display adaptor card 345)
- Electronic equipment 395 (GPS receiving module) by which a microprocessor receives current positional information through the interface unit 365 from magnetic-disk drive 370 and the worldwide positioning system in which read-out/writing is possible
[0016] In addition, it cannot be overemphasized that many components can be provided. For example, a portable computer can possess CD-ROM drive 380 and a floppy disk drive (FDD) 370, and these drives interface with the disk interface controller 364. Furthermore, in order to carry out rapid access of the data to a microprocessor from a disk drive, L2 cache 385 can also be provided and the slot of PCMCIA390 can also be provided as an object for circumference elements.
[0017] In other operation gestalten of the computer system of this invention this computer system The microprocessor which detects the input from an input device, and the memory in which writing/read-out are possible, [microprocessor] It has the receiver received in the I/O circuit connected to the microprocessor, and at least one worldwide positioning system. It becomes at least one component of this worldwide positioning system from the locator device which radiocommunicates current positional information. It is characterized by being programmed so that computer system impossible-izes at least one moving function alternatively based on current positional information.
[0018] In the example of further others of the computer system of this invention The microprocessor to which this computer system detects the input from an input device, The I/O circuit connected with the memory in which writing/read-out is possible by the microprocessor at the microprocessor, It has the receiver received in at least one worldwide positioning system. It becomes at least one component of this worldwide positioning system from the locator device which radiocommunicates current positional information. It is characterized by being programmed so that computer system enables activation of at least one encryption algorithm alternatively based on current positional information.
[0019] In the operation gestalt besides the computer system of this invention At least one microprocessor to which this computer system detects the input from an input device, The I/O circuit connected with the memory in which writing/read-out is possible by the microprocessor at the microprocessor, It has the receiver received in at least one worldwide positioning system. It becomes at least one component of this worldwide positioning system from the locator device which radiocommunicates current positional information. A microprocessor has the maximum performance beyond the 1st value based on a computer performance criterion, and is characterized by being restricted to the mode of low performance smaller than the 1st value.
[0020] or [that this approach enables activation of actuation of the function of a computer in the approach of impossible-izing the function of the computer of this invention alternatively based on the location data (b) thought to be the step which receives location data from (a) locator device] -- or it is characterized by to consist of a step of which activation is made impossible. In the approach of operating the computer of this invention, this approach is characterized by consisting of a step which restricts the maximum performance of a computer to below the 1st value specified according to the computer performance criterion based on the location data (b) Thought to be the step which receives location data from (a) locator device.
[0021] In the suitable operation gestalt, in order to prevent the error in a border zone, it has the margin of MAERA. In order to eliminate the possibility of an unjust country judging, the lookup stage contains the safety margin (namely, in order to prevent permitting an encryption process unsuitably). A non-GPS positioning system can also be used for the system of this invention, and it is usable in non-GPS systems, such as Roland (LORAN), an eagle eye, the Russia army satellite positioning system, or other

LEOS positioning systems. In order to prevent overcoming a safeguard when a user emulates GPS data, it is suitable for a system to provide a security function. For example, it is desirable to require as making a user sometimes move a system, and to have the process at which GPS data are changed. Thereby, the emulation by hardware can be made more into difficulty.

[0022] As for the above-mentioned security function, it is desirable it is not only applicable about coding, but that it is applicable about double sign-ization. Even if a message is unlawfully enciphered for some countries, it is because it may be possible (or impossible) legally to double-sign-ize the message enciphered legally. The above-mentioned safety function not only prevents illegal export of the version which can operate the managed software, but can prevent illegal import.

[0023] Since there is a legal demand needed for encryption, especially the problem relevant to the system which contains encryption software is very difficult. However, in this invention, such a problem can also be coped with and, moreover, it can apply also to the software of other types. For example, the open person of software has the case where he wants to sell the item which is equipped with a domestic license and has software. This is usually performed in sale of a book and is because it becomes possible to sell at a different price in a different country.

[0024] This invention is applicable to the software actuation for which a special order was given to a different country or the market of an area again. For example, various software parameters like the various clock frequency in a radiotelephony communication link can be made to correspond to the location data searched from the locator device automatically. This invention is applicable also in order to drive alternatively further two or more hardware peripheral devices. Therefore, in this domestic one, actuation of the component of the wireless which is not permitted in a specific country can be made impossible.

[0025] This invention cannot be applied only to the system based on the x86-party tsi bull microprocessor, and can be applied also to the system usingx[680] 0, RISC, or other processor architecture. In a multiprocessor system, this invention is used in order that the exclusive control processor which a user cannot program may communicate with a locator module, and a software function can be used for it that actuation is possible or in order to make it un-operating.

[0026] This invention cannot necessarily be applied only to the system which uses uniprocessor CPU, and the computer which uses the multiprocessor architecture can also be made to possess it. This invention cannot necessarily be applied only to a single user desktop system, and can be applied also to a Network Server, a main frame transaction processing system, a terminal, an engineering workstation, and a portable computer.

[0027] This invention can be influenced by import and the exporting method, and can take a separate gestalt in relation to a design and an implementation means. This invention can also apply LAN/WAN cinae flos rear **. Connection or embedding is possible for a GPS locator device to a LAN server, and it can perform alternatively whether it is a code, without the network which consists of two or more users using each user machine which needs a GPS locator device. By this configuration, cost can be sharply reduced in the company which has many computer users. When LAN is extended to a wide range field, in order to address in the exact location of GPS, additional software is needed on a user machine and a server.

[0028] In the computer system of this invention, a user input device can be equipped with the input means or other input means for a trackball joy stick, a three-dimension location sensor, and speech recognition as an option. An output device can be equipped with a loudspeaker, a display (or only display driver), a modem, or other output means. Furthermore, the embedding mold GPS receiver equipped with the electronic key circuit is also incorporable. In addition, it cannot be overemphasized that various deformation and modification are possible.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－161486

(43)公開日　平成11年(1999)６月18日

(51)Int.Cl.⁶		識別記号	ＰＩ		
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｃ
Ｇ０１Ｓ	5/14		Ｇ０１Ｓ	5/14	
Ｇ０６Ｆ	1/00	３７０	Ｇ０６Ｆ	1/00	３７０Ｅ

審査請求　未請求　請求項の数44　ＯＬ　（全９頁）

(21)出願番号　特願平10－245272

(22)出願日　平成10年(1998)８月31日

(31)優先権主張番号　９２０３８３

(32)優先日　1997年８月29日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591030868
コンパック・コンピューター・コーポレーション
COMPAQ COMPUTER CORPORATION
アメリカ合衆国テキサス州77070，ヒューストン，ステイト・ハイウェイ　249，20555

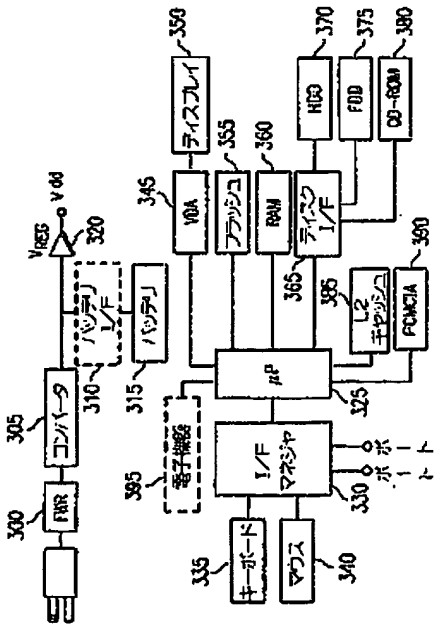
(72)発明者　サンボン・ピー・オラリグ
アメリカ合衆国テキサス州77429，サイプレス，エバーグリーン・ノウル・レイン　15415

(74)代理人　弁理士　社本　一夫　（外５名）

最終頁に続く

(54)【発明の名称】　コンピュータ・システム

(57)【要約】
【課題】　コンピュータの機能を国／地域によって限定的に動作させることができるようにする。
【解決手段】　コンピュータに電源が投入されると、ＧＰＳ等の位置決めシステムとの無線通信により、ロケータ・デバイスである電子機器３９５が、コンピュータの現在の位置を検出する。マイクロプロセッサ３２５は、位置に依存して動作機能を制限されるようプログラムされており、電子機器からの現在の位置データに基づいて、所定の機能を動作可能状態又は動作不能状態に設定する。また、電子機器をコンピュータから遮断した場合には、コンピュータ全体が動作不能となる。これにより、所定の機能が不許可の国／地域において、その機能を強制的に不能化することができる。



1

【特許請求の範囲】

【請求項１】　コンピュータ・システムにおいて、

入力デバイスからの入力を検出するマイクロプロセッサと、

マイクロプロセッサにより書き込み／読み出し可能なメモリと、

マイクロプロセッサに接続された入出力回路と、

少なくとも１つのワールドワイド位置決めシステムにおいて受信される受信機を有し、該ワールドワイド位置決めシステムの少なくとも１つの構成要素に現在の位置情報を無線通信するロケータ・デバイスとからなり、該コンピュータ・システムが、現在の位置情報に基づいて、少なくとも１つの動作機能を選択的に不能化するようにプログラムされていることを特徴とするコンピュータ・システム。

【請求項２】　請求項１記載のコンピュータ・システムにおいて、動作機能は、ソフトウエア・アプリケーションであることを特徴とするコンピュータ・システム。

【請求項３】　請求項１記載のコンピュータ・システムにおいて、動作機能は、暗号化アルゴリズムを含んでいることを特徴とするコンピュータ・システム。

【請求項４】　請求項１記載のコンピュータ・システムにおいて、動作機能は、ハードウエアによる演算機能であることを特徴とするコンピュータ・システム。

【請求項５】　請求項１記載のコンピュータ・システムにおいて、ワールドワイド位置決めシステムは、グローバル・ポジショニング・システム（ＧＰＳ）であることを特徴とするコンピュータ・システム。

【請求項６】　請求項１記載のコンピュータ・システムにおいて、ロケータ・デバイスは、該デバイスがコンピュータ・システムから取り除かれたときに、コンピュータ・システムが動作不能状態になることを特徴とするコンピュータ・システム。

【請求項７】　請求項１記載のコンピュータ・システムにおいて、該コンピュータ・システムは、位置データにエラーの空間マージンを適用するようにプログラムされており、これにより、コンピュータが国境近傍に存在するときに生じる可能性があるエラーを、その動作の前に防止することを特徴とするコンピュータ・システム。

【請求項８】　コンピュータ・システムにおいて、

入力デバイスからの入力を検出するマイクロプロセッサと、

マイクロプロセッサにより書き込み／読み出し可能なメモリと、

マイクロプロセッサに接続された入出力回路と、

少なくとも１つのワールドワイド位置決めシステムにおいて受信される受信機を有し、該ワールドワイド位置決めシステムの少なくとも１つの構成要素に現在の位置情報を無線通信するロケータ・デバイスとからなり、該コンピュータ・システムが、現在の位置情報に基づいて、

2

少なくとも１つの暗号化アルゴリズムを選択的に実行可能とするようプログラムされていることを特徴とするコンピュータ・システム。

【請求項９】　請求項８記載のコンピュータ・システムにおいて、暗号化アルゴリズムは、５６ビット以上の暗号を使用していることを特徴とするコンピュータ・システム。

【請求項１０】　請求項８記載のコンピュータ・システムにおいて、暗号化アルゴリズムは、符号化アルゴリズムであることを特徴とするコンピュータ・システム。

【請求項１１】　請求項８記載のコンピュータ・システムにおいて、ワールドワイド位置決めシステムは、グローバル・ポジショニング・システム（ＧＰＳ）であることを特徴とするコンピュータ・システム。

【請求項１２】　請求項８記載のコンピュータ・システムにおいて、ロケータ・デバイスがコンピュータ・システムから取り除かれたときに、コンピュータ・システムが動作不能状態になることを特徴とするコンピュータ・システム。

【請求項１３】　請求項８記載のコンピュータ・システムにおいて、ロケータ・デバイスは、コンピュータのシステム・ボードに一体化されていることを特徴とするコンピュータ・システム。

【請求項１４】　請求項８記載のコンピュータ・システムにおいて、マイクロプロセッサは、位置データにエラーの空間マージンを適用するようにプログラムされており、これにより、コンピュータが国境近傍に存在するときに生じる可能性があるエラーを、その動作の前に防止することを特徴とするコンピュータ・システム。

【請求項１５】　コンピュータ・システムにおいて、

入力デバイスからの入力を検出する少なくとも１つのマイクロプロセッサと、

マイクロプロセッサにより書き込み／読み出し可能なメモリと、

マイクロプロセッサに接続された入出力回路と、

少なくとも１つのワールドワイド位置決めシステムにおいて受信される受信機を有し、該ワールドワイド位置決めシステムの少なくとも１つの構成要素に現在の位置情報を通信するワイアレス・ロケータ・デバイスとからなり、マイクロプロセッサは、その最大パフォーマンスがコンピュータ・パフォーマンス（性能）標準に基づいている第１の値以上であり、かつ、第１の値よりも低パフォーマンスのモードに制限されていることを特徴とするコンピュータ・システム。

【請求項１６】　請求項１５記載のコンピュータ・システムにおいて、該コンピュータ・システムは４以上の複数のマイクロプロセッサを具えていることを特徴とするコンピュータ・システム。

【請求項１７】　請求項１５記載のコンピュータ・システムにおいて、複数のマイクロプロセッサは並列処理ア

ーキテクチャを構成するように接続されていることを特徴とするコンピュータ・システム。

【請求項18】 請求項15記載のコンピュータ・システムにおいて、ワールドワイド位置決めシステムは、グローバル・ポジショニング・システムであることを特徴とするコンピュータ・システム。

【請求項19】 請求項15記載のコンピュータ・システムにおいて、ワールドワイド位置決めシステムは、ディファレンシャル・グローバル・ポジショニング・システムであることを特徴とするコンピュータ・システム。

【請求項20】 請求項15記載のコンピュータ・システムにおいて、ロケータ・デバイスは、コンピュータの内部に一体化されており、かつ、該デバイスがコンピュータ・システムから取り除かれたときに、コンピュータ・システムが動作不能状態となることを特徴とするコンピュータ・システム。

【請求項21】 請求項15記載のコンピュータ・システムにおいて、ロケータ・デバイスは、コンピュータのシステム・ボードにマイクロプロセッサとともに一体化されていることを特徴とするコンピュータ・システム。

【請求項22】 コンピュータの機能を選択的に不能化する方法において、

(a) ロケータ・デバイスから位置データを受信するステップと、

(b) 受け取った位置データに基づいて、コンピュータの機能を動作可能にするか又は動作不能にするステップとからなることを特徴とする方法。

【請求項23】 請求項22記載の方法において、ロケータ・デバイスは、グローバル・ポジショニング・システム受信機であることを特徴とする方法。

【請求項24】 請求項22記載の方法において、ロケータ・デバイスは、デファレンシャル・グローバル・ポジショニング・システムの動作とコンパチブルであることを特徴とする方法。

【請求項25】 請求項22記載の方法において、コンピュータの機能は、ソフトウエア機能であることを特徴とする方法。

【請求項26】 請求項22記載の方法において、コンピュータの機能は、ハードウエア機能であることを特徴とする方法。

【請求項27】 請求項22記載の方法において、コンピュータの機能は、暗号化アルゴリズムの実行のためのアプリケーション要求であることを特徴とする方法。

【請求項28】 請求項22記載の方法において、コンピュータの機能は、ある位置でのみ許可されているソフトウエア・アプリケーションであることを特徴とする方法。

【請求項29】 請求項22記載の方法において、ステップ(b)は、電源投入時の自己テスト工程に含まれていることを特徴とする方法。

【請求項30】 請求項22記載の方法において、ステップ(b)は、コンピュータが国境近傍に存在するときに生じる可能性があるエラーを防止するために、位置データにエラーの空間マージンを提供することを特徴とする方法。

【請求項31】 請求項22記載の方法において、ロケータ・デバイスは、無線受信機であることを特徴とする方法。

【請求項32】 請求項22記載の方法において、ロケータ・デバイスは、コンピュータの内部に一体化されており、かつ、ロケータ・デバイスがコンピュータから取り除かれたときに、コンピュータが動作不能になるように接続されていることを特徴とする方法。

【請求項33】 請求項22記載の方法において、ロケータ・デバイスは、コンピュータのシステム・ボードに一体化されており、かつ、ロケータ・デバイスがコンピュータから取り除かれたときに、コンピュータが動作不能になるように接続されていることを特徴とする方法。

【請求項34】 コンピュータを動作させる方法において、

(a) ロケータ・デバイスから位置データを受信するステップと、

(b) 受け取った位置データに基づいて、コンピュータ・パフォーマンス(性能)標準によって規定された第1の値以下に、コンピュータの最大パフォーマンスを制限するステップとからなることを特徴とする方法。

【請求項35】 請求項34記載の方法において、ステップ(b)は、電源投入時の自己テスト工程に含まれていることを特徴とする方法。

【請求項36】 請求項34記載の方法において、ロケータ・デバイスは、グローバル・ポジショニング・システムの信号フォーマットとコンパチブルであることを特徴とする方法。

【請求項37】 請求項34記載の方法において、ステップ(b)は、コンピュータが国境近傍に存在するときに生じる可能性があるエラーを防止するために、位置データにエラーの空間マージンを提供することを特徴とする方法。

【請求項38】 請求項34記載の方法において、コンピュータは4以上の複数のマイクロプロセッサを含んでいることを特徴とする方法。

【請求項39】 請求項38記載の方法において、複数のマイクロプロセッサは、並列処理アーキテクチャを構成するように接続されていることを特徴とする方法。

【請求項40】 請求項34記載の方法において、コンピュータ・パフォーマンス標準は、コンピュータ・セオレティカル(理論)・パフォーマンス標準であることを特徴とする方法。

【請求項41】 請求項34記載の方法において、ロケータ・デバイスは、無線受信機であることを特徴とする

方法。

【請求項４２】 請求項３４記載の方法において．ロケータ・デバイスは、グローバル・ポジショニング・システムであるワールドワイド位置決めシステムであることを特徴とする方法。

【請求項４３】 請求項３４記載の方法において．ロケータ・デバイスは、無線受信機であり．コンピュータの内部に一体化されており．かつ、ロケータ・デバイスがコンピュータから取り除かれたときに．コンピュータが動作不能になるように接続されていることを特徴とする方法。

【請求項４４】 請求項３４記載の方法において．ロケータ・デバイスは、無線受信機であり．かつ、コンピュータのシステム・ボードに一体化されていることを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の技術分野】本発明は、コンピュータ・システムに関し、特に．国／地域確認のためにグローバル・ポジショニング・システム（ＧＰＳ）を用いて、コンピュータの暗号化機能を許可することができるコンピュータ・システム及びその方法に関する。

【０００２】

【従来の技術】ＧＰＳは．アメリカ政府の保有する複数のサテライトの集合であり．ワールドワイドで２４時間．位置情報及びナビゲーション情報を、極めて高精度に提供するものである。３以上のサテライトを捕捉することによって．ＧＰＳ受信機は自身の正確な位置を検出することができる。ＧＰＳは最も広範囲でかつ極めて正確なシステムであるが、他のサテライト・ポジショニング・システムもまた存在している。１９９７年に．アメリカ政府は、重要な暗号化技術の輸出を禁止することによって、アメリカのハイテクノロジ・ビジネスに足枷を掛けた。これにより、アメリカの企業は、暗号化技術の販売が法的に制限されていない外国の競争企業に比べて．販売金額がかなり減少している。このような販売金額の低減は、独占的な経済情報の盗聴によっても生じるものであり、このような経済情報は．強力な暗号化技術が輸出されて広範囲で用いられた場合には、十分に保護されるべきものである。

【０００３】しかしながら．アメリカだけが制限的な法律を有している訳ではない。例えば．フランスは．ライセンスを得ていない限り暗号化製品の輸入を禁止しており．そして、該ライセンスは簡単には得られないものである。制限的な法律を有している他の国々としては、ロシア．中国、ブラジル、シンガポール等を上げることができる。米国の輸出に関する法律は．高性能コンピュータ及びそれに類似する装置の輸出も制限している。ただし．この場合．該装置の処理能力がコンピュータ・セオレティカル（理論）・パフォーマンス（ＣＴＰ）標準に規定するレベル以上の場合に、輸出が制限されるものである。現在、２００以上のＣＴＰを有するシステムは、多数の外国に輸出することが禁じられている。しかしながら．このようなＣＴＰ標準は、今日の小型コンピュータの処理能力が飛躍的に増大することにより、ハイエンド・ワークステーション及びホーム・コンピュータに、直ぐに追いつかなくなってしまうと考えられる。

【０００４】輸出制限の法律によって生じる他の問題は．ダウンストリーム・トランスファ（下流転送）を効果的に制御することができない点である。すなわち、許可された外国へ輸出されたシステムが．製造者の知らない間に、不許可の外国へ再度輸出されてしまうという危険性がある。輸出に関する制限は、厄介であるだけでなく変化するものである。例えば、Commerce Departmentは最近、米国企業がキー復元製品を開発するための工程をデモンストレーションできる場合は．該企業はデータ暗号化標準（ＤＥＳ）の５６ビット暗号化製品を輸出することができることを提案した。しかしながら．キー復元製品が導入されたときには、政府は．キー復元処理が保証されたときに該処理を公開すべきであると．要求している。あるカスタマにとって、キーを他の企業等に提供することは．該企業からキーの機密性が損なわれてしまう等のリスクを生じることになる。したがって．政府の要求は、技術の開発意欲を低下させる原因になっている。

【０００５】他の公知の暗号化製品は．Pretty Good Privacy（ＰＧＰ）であり、これは．２０４８ビットまでの暗号を提供する。これは．一種の公開キー製品であり．メッセージの伝送においては、機密キーの変換を必要としていない。ＰＧＰは．認可とメッセージ伝送との両方に、強力なアルゴリズムを有している。送信側は、受信側が自由に公開できる一意的な公開キーを用いて、メッセージを暗号化する。受信側では．メッセージを解読するために．該受信側に一意的な機密キーを使用する。送信側の機密キーを用いてメッセージを暗号化することも可能であり、これにより、送信側の公開キーを知っている人はだれでも、メッセージを解読することができることになる。このことは、ビジネス取引及び個人的取引において広く使用されているデジタル署名を生成するために、重要なことである。米国特許第５６３５９４０号（Ｈｉｃｋｍａｎ等）には、モデムの位置依存動作について示唆を与えている。この米国特許は、モデムの位置を決定するための機構を含んだモデムを開示している。位置に依存して、装置の通信部分が再度環境設定されて．その位置での動作に必要な設定状態になる。

【０００６】

【発明の概要】本発明のコンピュータ・システムは、国／地域の確認のために具備されたＧＰＳハードウエアを用い．関連する制限法律に応じて、暗号化エンジン／アルゴリズムの選択的な制御を可能にしている。本発明の

システムの利点は、エンド・ユーザから離れた位置で認可キーの制御を行うことができることである。例えば、コンピュータにインストールされたソフトウエア暗号化アプリケーションは、GPSハードウエアからGPS情報を得て、システムの位置が暗号化の特定レベルからみて許可できる位置にあるかどうかを判定する。GPSを用いて、ユーザ位置の正確な読み取りを行うことができる。そのマシンに具備されている特定の暗号化製品が、例えば、米国内のみにその使用が制限されており、そして、GPSによって認定された位置が米国内である場合は、強力レベルで暗号化が許可される。しかしながら、暗号化製品が強力レベルでの暗号化が認可されていない場所に存在すると判定された場合は、暗号化機能は自動的に機能ダウンされ、または連邦の輸出制限規定に合致するように不能化される。

【0007】本発明のシステムの他の利点は、輸出が制限されているパワフル・コンピュータのダウンストリーム・トランスファを制御するために使用できることである。例えば、最大能力以上である複数のプロセッサ能力を有するコンピュータは、幾つかの特定の国には輸出が制限されている。このような能力を有するコンピュータが不許可の国内に位置している場合、プロセッサの能力は法律に合致したレベルに低下されるか、又は不能化される。本発明の更に他の利点は、組織的なカスタマにおいて、特定位置のユーザが、該組織のコンピュータ管理者によって特定されたソフトウエア・アプリケーションをインストールすることができることである。

【0008】好適な実施例においては、米国輸出ライセンス要求が単一タイプの認可に合致すればよい。上記した位置依存性のあるセキュリティ機能は、位置データに限定されているソフトウエア（又は、ハードウエア）が、禁止された位置において動作することを不可能にしているので、動作不可能なソフトウエア（又は、ハードウエア）がシステム内に組み込まれていることはあっても、動作可能なソフトウエア（又は、ハードウエア）は輸出されないことになる。したがって、あるタイプの認可が一旦出されると、位置依存のソフトウエアの新バージョン（又は、位置依存の新周辺装置）の個々の認可を必要としない。したがって、ソフトウエアのアップグレード（又は、新しい周辺装置）が、マーケットに素早く販売されることになる。

【0009】

【発明の実施の態様】GPSシステムは、正確な位置情報を提供するために、軍隊で最初に使用されるよう構成された。GPS製品は、戦場の兵士及び装備の位置を検出しかつそれらの移動を追尾して、海上の軍艦に報告し、かつ位置情報及びナビゲーション情報を軍隊の飛行機に提供するために、軍隊によって使用された。今日、GPS製品は、多数の商業的アプリケーション用として、開発されている。商業的アプリケーションとして、

測量及び地図作成、空中及び海上でのナビゲーション、車両追尾システム、及びモバイル・コンピュータ及びセルラ・プラットフォーム等を上げることができる。

【0010】極めて高精度の原子クロックを用いても、位置決定のプロセスには、ある程のエラーが生じてしまう。さらに、Selective Availability（SA）は、米国の国防省によって作成されたプログラムであり、該プログラムは、セキュリティ目的で、軍隊ではないユーザに対しては故意に、GPSがさほど正確ではないようにしている。SAを用いたことにより、位置の正確さは30～100メートル範囲程度の正確さである。SAを用いない場合でも、他のエラーが生じてしまう。これらのエラーの内で最も重大なものは、地球の電離層の変動によるものであり、該電離層の変動は、GPS無線信号の速度に影響を及ぼすものである。エラー発生の他の原因は、地球表面の大気圏における水蒸気によるものである。これらのエラーはともに、極めて小さいものである。GPSの精度は、ディファレンシャルGPS（DGPS）機能を用いて、近傍に固定されたDGPSビーコン受信機からの基準信号を読み取ることによって、改善される。

【0011】簡単に言えば、ソフトウエアとハードウエアとの間の相互作用は、図1及び図2に示されているように、以下の方法で行われる。まず、ユーザがシステムに電源投入する。システムのPOST処理が実行され、すべてのハードウエアの状態がチェックされる。特に、GPS受信回路が動作状態である場合、GPSデータは処理されて格納され、そして、ソフトウエアが実行されて要求が発生されるのを待機する。ソフトウエア要求を受信しない場合は、ハードウエア・ファームウエア・プログラムがソフトウエア要求を継続的にチェックする。その後、ソフトウエアが完全にロードされて暗号化プログラムを実行すると、ハードウエアにソフトウエア要求を送信しかつ該要求が送信されたことを確認するループ処理を開始する。ハードウエアがソフトウエア要求を受信すると、該要求を処理して、該要求が認証されたかどうかチェックする。要求が認証されている場合、暗号化が許可される。どのような理由であれ、ハードウエア・ファームウエアが、有効ではない位置が検出されたことをソフトウエアに報告すると、ソフトウエアは、有効な位置情報を要求するプログラムをシャットダウンすることを決定する。

【0012】図1は、電源投入から暗号化を開始するためのGPSハードウエア制御フローを示している。この処理は、ステップ100において、GPS装置にパワーアップすなわち電源投入することにより開始され、そして、ステップ105において、すべてのシステムの状態をチェックする。パワーアップ後に任意のシステムが障害発生を報告した場合、処理はステップ110の任意の暗号化を不能化する。すべてのシステムが動作可能であ

ることを報告した場合、ステップ１１５において、特定の送信機の位置が、ＧＰＳシステムによって確認され送信される。位置が送信された後、ステップ１２０において、システムはユーザからのアプリケーション要求（ＡＰＰ要求）信号を待機する。そして、ステップ１２５において、要求がまだ受信されていないと判定すると、処理はステップ１０５に戻って状態チェックを行い、要求がターゲットすなわちユーザから受信されるまで、このループ処理を実行する。要求を受信すると、ステップ１３０において、要求が有効な要求であるかどうかを検出するために、要求を前処理する。そして、ステップ１３５において、要求が有効でないと判定されると、ステップ１０５に戻って状態チェックを行い、そして、上記したステップを反復実行する。要求が有効である場合、認可コードがターゲットに返送され、ステップ１４０において、アプリケーションの暗号化が許可され実行される。処理ループは、所定の時間間隔で継続され、ターゲットの状態を更新してターゲットが動作可能であるかどうかを継続的に確認する。

【００１３】図２は、認証処理の間に実行されるソフトウエア・アルゴリズムである。ステップ２００において、アプリケーションの状態（ＡＰＰ状態）が確認され、適切に処理されるようにする。ステップ２０５において、ソフトウエアは、ＧＰＳハードウエアに対するハードウエアを要求する。ステップ２１０において、ＧＰＳハードウエアが動作不能であると判定した場合、ステップ２１５に移行し、ＧＰＳシステムが使用されていないことを、ターゲット・ユニットが判定する。ただし、この際、暗号化又はその他の特定の機能を除いて、制限された動作が実行される。ＧＰＳハードウエアが検出されて動作可能である場合、ステップ２２０に進んで、適切なソフトウエア・オプションが特定のターゲット・ユニットのために選択される。そして、ステップ２２５において、マスタ・ユニットへ送信するために、要求がハードウエアに送信される。ステップ２３０において、要求が適切に処理されたと判定した場合は、この処理は終了し、処理されなかった場合は、ステップ２３５において、エラー処理ルーチンを実行する。

【００１４】図３は、本発明の新規な暗号化方法を実行するポータブル・コンピュータ・システムを示している。システムは、バッテリを充電するパワーコンバータ３０５を備えている。バッテリとその他の回路との間にバッテリ・インターフェース（Ｉ／Ｆ）３１０を具備することが好ましい。パワー・コンバータ３０５は、ＡＣ主電源から全波整流器（ＦＷＲ）３００を介して電力が供給され、バッテリ３１５にＤＣ電圧を提供する。バッテリ３１５（又はコンバータ３０５）は、電圧レギュレータ３２０を介して、ポータブル・コンピュータ・システムにＤＣ電源Ｖｄｄを供給する。ポータブル・コンピュータ・システムは、例えば、以下の構成要素を具えている。

【００１５】・ユーザ入力デバイス（キーボード３３５及びマウス３４０）

・少なくとも１つのマイクロプロセッサ３２５［該マイクロプロセッサは、インターフェース管理チップ３３０を介して、入力デバイスから入力を受信する。なお、インターフェース管理チップもまた、種々のポートへのインターフェースを提供する。］

・マイクロプロセッサがアクセス可能なメモリ（フラッシュ・メモリ３５５及びＲＡＭ３６０）

・マイクロプロセッサが発生したデータを出力するデータ出力デバイス（ディスプレイ３５０及びビデオ・ディスプレイ・アダプタ・カード３４５）

・マイクロプロセッサがインターフェース・ユニット３６５を介して読み出し／書き込み可能な磁気ディスク・ドライブ３７０

・ワールドワイド位置決めシステムから現在の位置情報を受信する電子機器３９５（ＧＰＳ受信モジュール）

【００１６】その他多数の構成要素を具備することができることは言うまでもない。例えば、ポータブル・コンピュータは、ＣＤ－ＲＯＭドライブ３８０及びフロッピ・ディスク・ドライブ（ＦＤＤ）３７０を具備することができ、これらのドライブは、ディスク・インターフェース・コントローラ３６４にインターフェースされる。さらに、マイクロプロセッサにディスク・ドライブからデータを高速アクセスするために、Ｌ２キャッシュ３８５も具備することができ、また、ＰＣＭＣＩＡ３９０のスロットも、周辺要素用として具備することができる。

【００１７】本発明のコンピュータ・システムの他の実施形態において、該コンピュータ・システムは、入力デバイスからの入力を検出するマイクロプロセッサと、マイクロプロセッサにより書き込み／読み出し可能なメモリと、マイクロプロセッサに接続された入出力回路と、少なくとも１つのワールドワイド位置決めシステムにおいて受信される受信機を有し、該ワールドワイド位置決めシステムの少なくとも１つの構成要素に現在の位置情報を無線通信するロケータ・デバイスとからなり、コンピュータ・システムが現在の位置情報に基づいて、少なくとも１つの動作機能を選択的に不能化するようにプログラムされていることを特徴としている。

【００１８】本発明のコンピュータ・システムのさらに他の実施例においては、該コンピュータ・システムは、入力デバイスからの入力を検出するマイクロプロセッサと、マイクロプロセッサにより書き込み／読み出し可能なメモリと、マイクロプロセッサに接続された入出力回路と、少なくとも１つのワールドワイド位置決めシステムにおいて受信される受信機を有し、該ワールドワイド位置決めシステムの少なくとも１つの構成要素に現在の位置情報を無線通信するロケータ・デバイスとからなり、コンピュータ・システムが現在の位置情報に基づい

て．少なくとも1つの暗号化アルゴリズムを選択的に実行可能にするようにプログラムされていることを特徴としている。

【0019】本発明のコンピュータ・システムの外の実施形態においては、該コンピュータ・システムは．入力デバイスからの入力を検出する少なくとも1つのマイクロプロセッサと．マイクロプロセッサにより書き込み／読み出し可能なメモリと．マイクロプロセッサに接続された入出力回路と、少なくとも1つのワールドワイド位置決めシステムにおいて受信される受信機を有し．該ワールドワイド位置決めシステムの少なくとも1つの構成要素に現在の位置情報を無線通信するロケータ・デバイスとからなり．マイクロプロセッサが．コンピュータ・パフォーマンス標準に基づいている第1の値以上の最大パフォーマンスを有し、第1の値よりも小さい低パフォーマンスのモードに制限されていることを特徴としている。

【0020】本発明のコンピュータの機能を選択的に不能化する方法においては．該方法は．（a）ロケータ・デバイスから位置データを受信するステップと．（b）受け取った位置データに基づいて、コンピュータの機能の動作を実行可能にするか又は実行不可能にするステップとからなることを特徴としている。本発明のコンピュータを動作させる方法においては、該方法は、（a）ロケータ・デバイスから位置データを受信するステップと．（b）受け取った位置データに基づいて、コンピュータ・パフォーマンス標準によって規定された第1の値以下にコンピュータの最大パフォーマンスを制限するステップとからなることを特徴としている。

【0021】好適な実施形態においては、国境ゾーンにおけるエラーを防止するために、マエラーのマージンを具えている。不当な国判定の可能性を排除するため（すなわち、暗号化プロセスを不適切に許可してしまうことを防止するため）に、ルックアップ・ステージは．セーフティ・マージンを含んでいる。非ＧＰＳポジショニング・システムもまた、本発明のシステムに使用することが可能であり．ローラン（ＬＯＲＡＮ）、イーグル・アイ．ロシア宣サテライト位置決めシステム、または他のＬＥＯＳ位置決めシステム等の非ＧＰＳシステムを使用可能である。ユーザがＧＰＳデータをエミュレートすることによってセーフガードを潜り抜けることを防止するために、システムにセキュリティ機能を具備されることが好適である。例えば、ユーザにシステムを時々移動させるよう要求して、ＧＰＳデータが変更されるようにする工程を具えることが好ましい。これにより、ハードウエアによるエミュレーションをより困難にすることができる。

【0022】上記したセキュリティ機能は、符号化について適用できるだけでなく．復号化についても適用できることが好ましい。国によっては、メッセージが不法に暗号化されたとしても、法的に暗号化されたメッセージを復号化することが法的に可能（又は不可能）である場合があるからである。上記したセーフティ機能は．管理されたソフトウエアの動作可能なバージョンの不法な輸出を防止するだけでなく．不法な輸入も防止することができる。

【0023】暗号化ソフトウエアを内蔵しているシステムに関連する問題は、暗号化に特に必要とされる法的な要求があるために極めて困難である。しかしながら、本発明においては．このような問題にも対処することができ．しかも他のタイプのソフトウエアにも適用することができる。例えば、ソフトウエアの公開者は、国内だけのライセンスを備えてソフトウエアのあるアイテムを販売したい場合がある。これは、本の販売において通常行われており、異なる国においては異なる価格で販売することが可能になるからである。

【0024】本発明はまた．異なる国又は地域のマーケットに対して特注されたソフトウエア動作に適用することができる。例えば、無線電話通信における種々の動作周波数のような種々のソフトウエア・パラメータを、ロケータ・デバイスから検索された位置データに自動的に対応させることができる。本発明はさらに、複数のハードウエア周辺機器を選択的にドライブするためにも適用することができる。したがって、特定の国で許可されていない無線の構成要素を．該国内では動作が不可能とすることができる。

【0025】本発明は、ｘ８６-コンパチィブル・マイクロプロセッサに基づくシステムだけに適用可能であるものではなく．６８０ｘ０．ＲＩＳＣ．又は他のプロセッサ・アーキテクチャを用いたシステムにも適用できる。本発明は．マルチプロセッサ・システムにおいて、ユーザがプログラム不能な専用コントロール・プロセッサが．ロケータ・モジュールと通信するために使用され．また、ソフトウエア機能を動作可能又は非動作にするために使用することができる。

【0026】本発明は、単一プロセッサＣＰＵを用いているシステムにだけ適用可能であるわけではなく．マルチプロセッサ・アーキテクチャを用いているコンピュータにも具備させることができる。本発明は、単一ユーザ・デスクトップ・システムだけに適用可能であるわけではなく、ネットワーク・サーバ、メインフレーム・トランザクション処理システム．端末、エンジニアリング・ワークステーション、及びポータブル・コンピュータにも適用可能である。

【0027】本発明は、輸入及び輸出法によって影響を受け．また、設計及び実現手段に関連して別々の形態をとることができるものである。本発明は、ＬＡＮ／ＷＡＮシナリアにも適用可能である。ＧＰＳロケータ・デバイスは、ＬＡＮサーバに接続又は埋め込み可能であり、複数のユーザからなるネットワークが．ＧＰＳロケータ

13

・デバイスを必要とする各ユーザ・マシンを使用することなく、選択的に暗号かを実行することができる。この構成により、多数のコンピュータ・ユーザを有する企業において、コストを大幅に低減させることができる。ＬＡＮがより広範囲の領域に拡張される場合、ＧＰＳの正確な位置にアドレス指定するために、ユーザ・マシン及びサーバ上に追加のソフトウエアが必要となる。

【００２８】本発明のコンピュータ・システムにおいては、ユーザ入力デバイスが、トラックボール・ジョイスティック、３次元位置センサ、音声認識用の入力手段、又は他の入力手段を、オプションで備えることができる。出力デバイスは、スピーカ、ディスプレイ（又は単＊

14

＊にディスプレイ・ドライバ）、モデム、又は他の出力手段を備えることができる。さらに、電子キー回路を備えた埋め込み型ＧＰＳ受信機も、組み入れることができる。その他、種々の変形、変更が可能であることは言うまでもない。

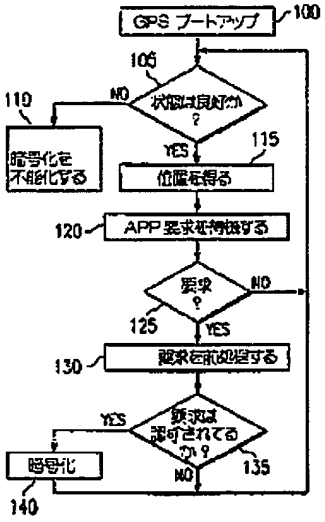
【図面の簡単な説明】

【図１】本発明に係るＧＰＳハードウエア制御のフローチャートである。

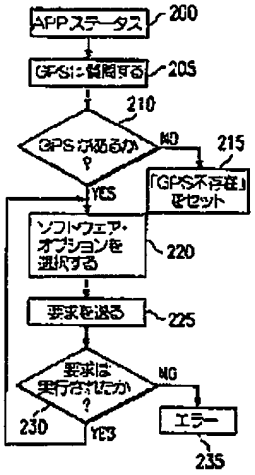
【図２】本発明に係るアプリケーション・ソフトウエアのフローチャートである。

【図３】本発明に係る埋め込まれたＧＰＳ電子機器を有するコンピュータ・システムのブロック図である。

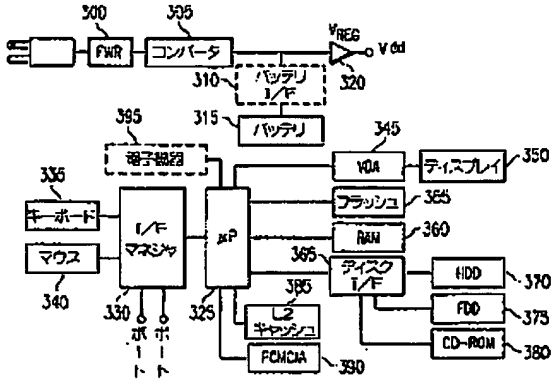
【図１】



【図２】



【図３】



フロントページの続き

(71)出願人 591030868
20555 State Highway 249, Houston, Texas 77070, United States of America

(72)発明者 ディレイス・エム・フリデル
アメリカ合衆国テキサス州77375, トンボール, ゲイツデン 11050, アパートメント 1914

(72)発明者 マイケル・エフ・アンジェロ
アメリカ合衆国テキサス州77068, ヒューストン, アンバー・フォレスト・ドライブ 3303